```
File 696:DIALOG Telecom. Newsletters 1995-2003/May 19
         (c) 2003 The Dialog Corp.
File   9:Business & Industry(R) Jul/1994-2003/May 19
         (c) 2003 Resp. DB Svcs.
File  15:ABI/Inform(R) 1971-2003/May 17
         (c) 2003 ProQuest Info&Learning
File  98:General Sci Abs/Full-Text 1984-2003/Apr
         (c) 2003 The HW Wilson Co.
File 484:Periodical Abs Plustext 1986-2003/May W2
         (c) 2003 ProQuest
File 553:Wilson Bus. Abs. FullText 1982-2003/Apr
         (c) 2003 The HW Wilson Co
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2003/May 20
         (c) 2003 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2003/May 17
         (c) 2003 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2003/May 20
         (c) 2003 Business Wire.
File 369:New Scientist 1994-2003/May W1
         (c) 2003 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2003/May 20
         (c) 2003 The Dialog Corp.
File  16:Gale Group PROMT(R) 1990-2003/May 19
         (c) 2003 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2003/May 16
         (c) 2003 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2003/May 19
         (c)2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2003/May 19
         (c) 2003 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2003/May 19
         (c) 2003 The Gale Group
File 624:McGraw-Hill Publications 1985-2003/May 19
         (c) 2003 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2003/May 16
         (c) 2003 San Jose Mercury News
File 636:Gale Group Newsletter DB(TM) 1987-2003/May 19
         (c) 2003 The Gale Group
File 647:CMP  Computer Fulltext 1988-2003/Apr W4
         (c) 2003 CMP Media, LLC
File 674:Computer News Fulltext 1989-2003/May W3
         (c) 2003 IDG Communications
? ds

Set     Items   Description
S1    6066173   KEY OR CIPHER??? ? OR CYPHER??? ? OR ALGORITHM??? ?
S2      22791   (SESSION? ? OR SUBSESSION? OR DATA OR CATEGORY OR ONE()TIM-
             E)(1W)S1
S3     170107   (PUBLIC OR TWO)(1W)S1 OR TWO()KEY? ? OR KEY()PAIR? ?
S4        416   ASYMMETRIC(1W)S1
S5      14083   (MASTER OR GROUP OR COMMON)(1W)S1
S6      19511   S2(5N)(DATA OR INFORMATION OR PACKET? ? OR MESSAGE? ? OR F-
             ILE OR FILES OR CONTENT)
```

S7 4 S2(S)S3:S4(S)S5
S8 1 S7/2000:2003
S9 3 S7 NOT S8
S10 3 RD (unique items)
? t10/3,k/all

10/3,K/1 (Item 1 from file: 696)
DIALOG(R)File 696:DIALOG Telecom. Newsletters

00615450
SUMMARY OF RESPONSES TO THE CONSULTATION PAPER
TELECOMMS FRAUD REVIEW
June 1, 1998 VOL: 2 ISSUE: 6 DOCUMENT TYPE: NEWSLETTER
PUBLISHER: PHILLIPS BUSINESS INFORMATION
LANGUAGE: ENGLISH WORD COUNT: 1080 RECORD TYPE: FULLTEXT

TEXT:
...attractive target.
* It was wrong to make the assumption that users would normally have separate **key pairs** for authentication and confidentiality.
* It was unclear whether a warrant would result in a **session key** being handed over or a **master key** of some kind. If the latter, then any time limit specified in the warrant could...

...with key escrow workable would involve an unacceptable degree of pioneering and complexity.
* In conventional **public key** systems, warranted access to a user's private confidentiality key would only enable encryption of...

10/3,K/2 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

02367353 117541446
Internet's information highway potential
De Maeyer, Dirk
Internet Research v7n4 PP: 287-300 1997
ISSN: 1066-2243 JRNL CODE: NTRS
WORD COUNT: 8297

...TEXT: Routing Protocol (BGRP) (Smith and Armitage, 1996) and so on.

Also heavily studied is the **public key** technology, with findings such as the Internet Security Association and Key Management Protocol (ISAKMP) (Maughan...

... 1996), the Simple Key management for Internet Protocols (SKIP) (Aziz et al., 1996), the Photuris **session key** management protocol (Karn and Simpson, 1996), the **Group Key** Management Protocol (GKMP) (Harney and Muckenhirm, 1996a; 1996b), the **public key** login protocol (Kemp, 1996) and the Exponential Security System (TESS) (Danisch, 1995), and the authentication...

10/3,K/3 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

00938834 95-88226
Cryptanalysis and protocol failures
Simmons, Gustavus J
Communications of the ACM v37n11 PP: 56-65 Nov 1994
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 7170

...TEXT: terminals have the capability to carry out the easy one of a complementary pair of **public key** (asymmetric) cryptographic operations (for example, forming a modular cube with respect to a composite modulus...

... single key (symmetric) cryptographic operation (for example, by forming the exclusive or of a binary **one - time key** with a binary text to implement unconditionally secure Vernam ciphers). (Figure 1 omitted) All terminals also have the capability to encrypt and/or decrypt messages using a network-wide **common** cryptographic **algorithm** , such as the digital encryption standard (DES).

Subscriber A, wishing to communicate securely with subscriber B, sends a (randomly chosen) **one - time key** encrypted under the easy end of the server's **public key** system to the server along with a request for the server to set up a secure channel to B. The server contacts B, who generates a (random) **session key** and encrypts it under the easy end of the server's **public key** system. B sends this cipher to the server. The server, which is able to do the hard task of decrypting cyphers in the **public key** system--in this case to take modular cube roots with respect to the composite modulus chosen,(3)decrypts both ciphers to recover the **session key** provided by B and the **one - time key** provided by A. He then Vernam-encrypts the **session key** with the **one - time key** by forming the exclusive or of their representation as binary numbers and sends the resulting cipher to A, who can decrypt it using the **one - time key** chosen initially to recover the **session key** . A and B now possess a **common key** they can use to communicate securely. An eavesdropper, on the other hand, will have seen three ciphers: the **session key** and the **one - time key** , each encrypted using the server's **public key** , and the Vernam encryption of the **session key** with a **one - time key** .

The object of the protocol seems to have been achieved. Terminals having very limited computational...
?

File 2:INSPEC 1969-2003/May W2
(c) 2003 Institution of Electrical Engineers
File 6:NTIS 1964-2003/May W3
(c) 2003 NTIS, Intl Cpyrght All Rights Res
File 8:Ei Compendex(R) 1970-2003/May W2
(c) 2003 Elsevier Eng. Info. Inc.
File 34:SciSearch(R) Cited Ref Sci 1990-2003/May W2
(c) 2003 Inst for Sci Info
File 35:Dissertation Abs Online 1861-2003/Apr
(c) 2003 ProQuest Info&Learning
File 65:Inside Conferences 1993-2003/May W2
(c) 2003 BLDSC all rts. reserv.
File 94:JICST-EPlus 1985-2003/May W3
(c)2003 Japan Science and Tech Corp(JST)
File 95:TEME-Technology & Management 1989-2003/May W1
(c) 2003 FIZ TECHNIK
File 99:Wilson Appl. Sci & Tech Abs 1983-2003/Apr
(c) 2003 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2003/May 16
(c) 2003 The Gale Group
File 144:Pascal 1973-2003/May W2
(c) 2003 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2003/May 14
(c) Information Today, Inc
File 233:Internet & Personal Comp. Abs. 1981-2003/Apr
(c) 2003 Info. Today Inc.
File 266:FEDRIP 2003/Mar
Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2003/May 19
(c) 2003 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 The Gale Group
File 603:Newspaper Abstracts 1984-1988
(c)2001 ProQuest Info&Learning

```
Set     Items   Description
S1    2343191   KEY OR CIPHER??? ? OR CYPHER??? ? OR ALGORITHM??? ?
S2      21135   (SESSION? ? OR SUBSESSION? OR DATA OR CATEGORY OR ONE()TIM-
             E)(1W)S1
S3      50117   (PUBLIC OR TWO)(1W)S1 OR TWO()KEY? ? OR KEY()PAIR? ?
S4        227   ASYMMETRIC(1W)S1
S5       3768   (MASTER OR GROUP OR COMMON)(1W)S1
S6      20597   S2(5N)(DATA OR INFORMATION OR PACKET? ? OR MESSAGE? ? OR F-
             ILE OR FILES OR CONTENT? ?)
S7         17   S2 AND S3:S4 AND S5
S8          7   S7/2000:2003
S9         10   S7 NOT S8
S10         8   RD (unique items)
S11         0   HW FILES
? t10/7/all
```

10/7/1 (Item 1 from file: 2)

DIALOG(R)File 2:INSPEC

6450319 INSPEC Abstract Number: C2000-02-6130S-023
Title: Group public key **agreement protocol**
Author(s): Barmawi, A.M.; Takada, S.; Doi, N.
Author Affiliation: Keio Univ., Japan
Conference Title: Proceedings of the Seventeenth IASTED International Conference. Applied Informatics p.654-7
Editor(s): Hamza, M.H.
Publisher: ACTA Press, Anaheim, CA, USA
Publication Date: 1999 Country of Publication: USA 699 pp.
ISBN: 0 88986 241 9 Material Identity Number: XX-1999-00795
Conference Title: Proceedings of 17th IASTED International Conference on Applied Informatics (AI'99)
Conference Sponsor: IASTED
Conference Date: 15-18 Feb. 1999 Conference Location: Innsbruck, Austria
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Many key agreement protocols have been proposed for establishing the **session key** between more than two users. These protocols are based on symmetric cryptography and verification must be done several times when verifying several signatures, thus increasing the computational burden for all users in the group. To reduce the computational burden, we propose an agreement protocol which is based on asymmetric cryptography and only one verification is necessary to verify several signatures. We call our protocol **group public key** agreement protocol. In the proposed protocol we split the group's secret key into several partial secret keys. Each user has one partial secret key which is used to sign a common message. (8 Refs)
Subfile: C

10/7/2 (Item 2 from file: 2)

DIALOG(R)File 2:INSPEC

6361410 INSPEC Abstract Number: B1999-11-6210L-015, C1999-11-6150N-006
Title: Decentralized group key **management for secure multicast communications**
Author(s): Peyravian, M.; Matyas, S.M.; Zunic, N.

Author Affiliation: IBM Corp., Research Triangle Park, NC, USA
Journal: Computer Communications vol.22, no.13 p.1183-7
Publisher: Elsevier,
Publication Date: 25 Aug. 1999 Country of Publication: Netherlands
CODEN: COCOD7 ISSN: 0140-3664
SICI: 0140-3664(19990825)22:13L.1183:DGMS;1-T
Material Identity Number: H089-1999-015
U.S. Copyright Clearance Center Code: 0140-3664/99/$20.00
Document Number: S0140-3664(99)00121-8
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)

Abstract: Multicast protocols provide mechanisms for a sender to send a message to multiple receivers simultaneously. When the multicast message is of a sensitive nature, it should be encrypted. This would require that all the members of the multicast group share the same encryption key. We present a simple and scaleable method to create and distribute symmetric cryptographic keys amongst a group of communicating network users for multicast communications. The group symmetric keys permit each user to conveniently and securely communicate, share and access data belonging to the multicast group. Unlike current **group key** -management mechanisms, this scheme does not involve the use of a centralized key distribution center-only the group members generate and distribute group symmetric keys. Once a long-term **group key** has been established among a group of communicating peers, the scheme provides an easy way for any group member to send secure messages to all other group members without having to send the **session key** individually to each group member. Moreover, the scheme provides an option for allowing data traffic to be authenticated on a per-sender basis with sender-specific keys. (10 Refs)

Subfile: B C

10/7/3 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

5904634 INSPEC Abstract Number: B9806-6120B-035, C9806-6130S-024
Title: Development of multi-modal encryption LSI
Author(s): Takata, S.; Matsumoto, H.; Kawakubo, S.; Yamanaka, K.
Journal: NTT R & D vol.47, no.2 p.25-30
Publisher: NTT,
Publication Date: 1998 Country of Publication: Japan
CODEN: NTTDEC ISSN: 0915-2326
SICI: 0915-2326(1998)47:2L.25:DMME;1-8
Material Identity Number: N541-98003
Language: Japanese Document Type: Journal Paper (JP)
Treatment: Applications (A); Practical (P)

Abstract: We have developed an LSI that prevents unauthorized users from reading encryption keys. This LSI is a single-chip computer containing a RISC-type CPU, flash-ROM and RAM. It supports secret-key cryptosystems, **public - key** cryptosystems, and message digest functions. It prevents the **session - key** of secret-key cryptosystems and the private-key of **public - key** cryptosystems being revealed while encryption, authentication, or signature algorithms are being executed. It can also, detect altered programs in the flash-ROM. Placing that function and the **master - key** in a capsule prevents illegal users from reading the keys. This chip also provides user authentication and works using context. We describe those characteristics of our LSI and propose an application to information distribution systems which trade commodities via the Internet. (5 Refs)

Subfile: B C

10/7/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

5093612 INSPEC Abstract Number: B9512-6120B-103, C9512-6130S-057
Title: A new key escrow system with active investigator
Author(s): Horster, P.; Michels, M.; Petersen, H.
Author Affiliation: Theor. Comput. Sci. & Inf. Security, Univ. of Technol. Chemnitz-Zwickau, Chemnitz, Germany
Conference Title: SECURICOM 95. 13th Worldwide Congress on Computer and Communications Security and Protection Proceedings p.15-27
Publisher: Manifestations & Commun. Int, Paris, France
Publication Date: 1995 Country of Publication: France 288 pp.
Conference Title: Proceedings of 13th Worldwide Congress on Computer and Communications Security and Protection. Securicom 95
Conference Date: 8-9 June 1995 Conference Location: Paris, France
Language: English Document Type: Conference Paper (PA)
Treatment: New Developments (N); Practical (P)
Abstract: We review the Escrow Encryption Standard and the escrowed key exchange protocol with active investigator presented recently. We point out the main weaknesses in both approaches and give an overview of proposed solutions, which have not always successfully achieved the requirements. We also present a new software based escrowed key exchange protocol with active investigator that copes with cryptographic weaknesses. Our approach is a step towards designing key escrow protocols which achieve only those requirements which are absolutely necessary for the escrow agency. The limit of escrowed key exchange protocols is that we can't avoid criminals using other channels to compute a **common key** or encrypting the **session key** again, e.g. using a secret hash function. (18 Refs)
Subfile: B C

10/7/5 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

04020704 INSPEC Abstract Number: B91078284, C91072218
Title: Cryptographic method and applications
Author(s): Takar, K.; Nakamura, T.
Author Affiliation: Syst. Dev. Lab., Hitachi Ltd., Japan
Journal: Joho Shori vol.32, no.6 p.714-23
Publication Date: 1991 Country of Publication: Japan
CODEN: JOSHA4 ISSN: 0447-8053
Language: Japanese Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: The authors cover: procedure open types; the Data Encryption Standard; RSA public keys; procedure secret types; the **common key cipher** algorithm; the **public key cipher** algorithm; the vernam cipher; FEAL-N (fast **data** encryption **algorithm** N); MULTI2 (multimedia encryption 2); known plaintext attack; ciphertext attack; cipher block chaining; and chosen plaintext attack. (29 Refs)
Subfile: B C

10/7/6 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

01998106 INSPEC Abstract Number: B83009014, C83009959
Title: Public - key **enciphering/deciphering transformations using a conventional algorithm**
Author(s): Lennon, R.E.; Matyas, S.M.; Meyer, C.H.
Author Affiliation: IBM Corp., Armonk, NY, USA
Journal: IBM Technical Disclosure Bulletin vol.25, no.3A p.1241-9
Publication Date: Aug. 1982 Country of Publication: USA
CODEN: IBMTAA ISSN: 0018-8689
Language: English Document Type: Journal Paper (JP)
Treatment: New Developments (N)
Abstract: A **data** -encrypting **key** (K) is enciphered under a variant (KMX) of a host **master key** (KM0), with the resulting encipherment, i.e. E/sub KMX/(K), being used only for enciphering data. (3 Refs)
Subfile: B C

10/7/7 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01195357 ORDER NO: AAD91-36136
DESIGN OF TIME DELAY NEURAL NETWORKS FOR SPEECH RECOGNITION
Author: BUHRKE, ERIC ROLFE
Degree: PH.D.
Year: 1991
Corporate Source/Institution: ILLINOIS INSTITUTE OF TECHNOLOGY (0091)
Adviser: JOSEPH L. LOCICERO
Source: VOLUME 52/07-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 3788. 247 PAGES

This thesis solves some of the design problems encountered when using time delay neural networks for speech recognition. Time delay neural networks are used for recognizing time varying patterns. Recognition is accomplished by converting time into a space where a multi-layer perceptron performs the classification.

Unlike other common speech recognition algorithms, time delay neural networks have no explicit scheme for time alignment. This disadvantage is alleviated by using a large multi-layer perceptron with a sliding analysis window. The multi-layer perceptron has powerful discrimination characteristics and is able to perform temporal alignment within the sliding window.

An important aspect of the time delay neural network design is the specification of its network weights. This process is called training. Training algorithms adjust the network weights to optimize a performance criterion over a set of training data. **Common** training **algorithms** converge very slowly and perform questionably on data that is not part of the training set.

This research introduces a new training algorithm that uses the statistical properties of the training **data** . This **algorithm** not only converges quickly, but generalizes well. Training time is demonstrated to be nearly an order of magnitude less than conventional learning techniques, like backpropagation.

Another novel technique, termed network fusion, is proposed for including a priori knowledge during the network design. This helps avoid sub-optimal solutions. Its realization fits well into the neural network framework.

An information theoretic solution to the thresholding problem associated with the time delay neural network is also studied in this thesis. The thresholds are adjusted to maximize the mutual information

between the threshold output and the utterance class. **Two algorithms** for solving this problem are presented.

The techniques developed here are applied to the design of a speech recognition system. Two speech recognition experiments are performed, one with a small Spanish vocabulary, and the other with a slightly larger English vocabulary. Both of these databases were recorded in real world environments. It is demonstrated that the statistical training and the network fusion are efficient design methodologies for these practical speech recognition problems.

10/7/8 (Item 1 from file: 94)

03833117 JICST ACCESSION NUMBER: 98A0986956 FILE SEGMENT: JICST-E

Conference Key Supervision in a Level-Based Hierarchy.

WANG C-T (1); CHANG C-C (1); LIN C-H (2)
(1) National Chung Cheng Univ., Chiayi, Twn; (2) Tunghai Univ., Taichung, Twn

IEICE Trans Fundam Electron Commun Comput Sci(Inst Electron Inf Commun Eng), 1998, VOL.E81-A,NO.10, PAGE.2219-2227, FIG.2, REF.23
JOURNAL NUMBER: F0699CAT ISSN NO: 0916-8508
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3 681.3.02-759 651.01
LANGUAGE: English COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication

ABSTRACT: In this paper, we propose a new conference key distribution scheme and the supervision of a conference when users are in a level-based hierarchy. In a conference key distribution system, one message is transmitted to the participants from a chairman, a legitimate member can decrypt it and reveal the **common session key** . The proposed scheme can be implemented without using any tamper-proof hardware. For users in a level-based hierarchy, by applying the key distribution scheme, the higher priority users can derive the conference key and supervise the lower level users' communications. Further, the users in the same level who are not members of the conference or in lower levels can not expose the conference key. To break the **common session key** , a malicious user has to suffer from the difficulty of factorization and discrete logarithm problems. (author abst.)

?

```
File 256:SoftBase:Reviews,Companies&Prods. 82-2003/Apr
         (c)2003 Info.Sources Inc
? ds

Set     Items   Description
S1       5516   KEY OR CIPHER??? ? OR CYPHER??? ? OR ALGORITHM??? ?
S2         66   (SESSION? ? OR SUBSESSION? OR DATA OR CATEGORY OR ONE()TIM-
              E)(1W)S1
S3        571   (PUBLIC OR TWO)(1W)S1 OR TWO()KEY? ? OR KEY()PAIR? ?
S4          2   ASYMMETRIC(1W)S1
S5         10   (MASTER OR GROUP OR COMMON)(1W)S1
S6         58   S2(5N)(DATA OR INFORMATION OR PACKET? ? OR MESSAGE? ? OR F-
              ILE OR FILES OR CONTENT)
S7          0   S2 AND S3:S4 AND S5
?
```

```
File 347:JAPIO Oct 1976-2003/Jan(Updated 030506)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200331
         (c) 2003  Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2003/Apr W04
         (c) 2003 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20030515,UT=20030508
         (c) 2003 WIPO/Univentio
? ds

Set     Items   Description
S1          0   AU='MIRE P'
S2         43   CO='DELL COMPUTER B V':CO='DELL CORPORATE SERV'
S3        244   CO='DELL'
S4     341442   KEY? ? OR CIPHER? OR CYPHER?
S5       9508   S4(3N)(SESSION? OR PUBLIC OR ASYMMETRIC? OR SYMMETRIC?)
S6          0   S2:S3 AND S5
```